Unclassified
Summer 2003
No. 83

Canadian Security Intelligence Service

Commentary

Intelligence After 9/11: A British View of the Effects

Michael Herman

Commentary reflects the personal view of the author(s) and does not imply CSIS authentication or endorsement.

Introduction

Not everyone was happy with President Bush's proclamation of the 'war on terrorism' after 11 September 2001 ('9/11'), but there is now not much doubt that Al Qaida has been at war against the United States since the attack on the World Trade Center in 1993, and that the rest of the 'capitalist West' (however defined) is now threatened as America's ally. At the time of writing (winter 2002-3) the British government is giving wide publicity to the threat of terrorist attack with chemical, biological or radiological weapons, and has warned the public that complete defence cannot be guaranteed. Assuming that this is well-founded, we live in a climate of serious threat, and one that will not be short-lived.

So intelligence's importance in combating terrorism can be taken as read. Its current place in American thinking was emphasized in President Bush's National Security Strategy of 20 September 2002: his eighteen references to intelligence as a prime national instrument were rivalled only by twenty-four to military means, and contrasted with seven to diplomacy. Most Western countries have followed the American example, and have increased intelligence's budgets and relaxed legal limitations on its activities. Everywhere it is riding high.

This has not been a complete reversal of a previous position. Intelligence had indeed been reduced as part of the peace dividend at the end of the Cold War, but budgets were already being increased before 9/11 to cope not only with terrorism but with the requirements of the 1990s to support international peace-enforcement and humanitarian operations, and for intelligence on WMD proliferation, sanctions evasion, drug trafficking and the other emerging targets of the decade. Governments were already adapting themselves to what seemed an increasingly unstable world, and to the revolution within it in the information available and governments' ability to collect and process it. Intelligence satellites had ceased to be a superpower preserve and were being operated or planned by a range of second-rank powers. Intelligence as a whole was becoming a rather more legitimate organ of state, no longer quite such a deniable activity.

But 9/11 dramatically reinforced the trend. It confirmed intelligence's position as a major attribute of national soft (or semi-soft) power; all nations except the smallest will soon develop it, if they do not have it already. It also highlighted the role of counter-terrorism within it. This can now be accepted as a distinct and important intelligence category, akin to the older political, military and economic subsets, and subsuming much of what has previously been labelled as 'security intelligence'. No doubt it will have competition from other requirements - the related search for 'smoking gun' evidence on Saddam Hussei's WMD developments is currently of equal priority in US eyes - but it seems set nevertheless to be a major, lasting influence on the intelligence community.

Intelligence is due to change radically in any case, as part of the information revolution of which it is an element. As two American writers put it before 9/11, 'if it is to remain effective, the intelligence community will have to change - so much, that when these changes are completed, it will likely bear little resemblance to the organization created fifty years ago'.[1] But counter-terrorism's central position within it in a lengthy quasi-war will give the process a particular spin.

This paper speculates on what this will be, and what issues it poses. It gives a personal British view, drawing largely on British experience plus recent American announcements; but with some application to 'Western' intelligence as a whole, and perhaps more widely.

Counter-terrorism and Intelligence's Character

Intelligence on terrorism (shortened here for convenience to 'counter-terrorism') is characteristically based on the identification and tracking of *people* and their plans and activities. Its targeting is on individuals rather than 'things', and contrasts with military intelligence's concentration on the *matériel* of military power and the order of battle of formed units. Its aim is detection, rather than the analysis of complete situations that marks much other intelligence, for example the battlefield 'situational awareness' made possible by the power of modern technical collection. For such reasons, much discussion of counter-terrorism before and after 9/11 has focused on the need for better Humint as the prime requirement.

This may have shown elements of naivety and the search for panaceas. Good human sources on terrorism are worth their weight in gold; British success in the battle against the IRA depended in large measure upon them. American commentators may indeed be correct in arguing that the CIA's Directorate of Operations became demoralized in the 1990s by persistent media and Congressional criticism and lack of managerial support. But it is unrealistic to pin too many hopes on even an enhanced Humint effort against such security-conscious targets.

Instead, counter-terrorism's most important and distinctive challenge may lie not in any particular kind of collection, but in searching for connections among many diverse kinds of evidence. A member of the British Security Service's International Counter Terrorist Branch has written recently about what is involved.[2] He argues that counterterrorism is neither playing chess against a single enemy nor completing a jigsaw puzzle, unless it is accepted that the picture is fragmentary and fleeting with many pieces in the box that fit nowhere. In the search for clues, he prefers a metaphor of tracing threads and weaving patterns. The raw material is itself variegated and extensive, including:

- secret intelligence such as the intercepted communications of known terrorists;
- secret intelligence on those, perhaps overseas, known to have been involved in terrorist support activity in the past;
- reports from overseas security organizations (again of highly variable quality and sometimes politically coloured) on actual or possible terrorist planning;

- police reports, for instance of suspicious movements through ports;
- allegations from 'walk-ins' who claim to have inside knowledge of terrorist plans;
- calls from members of the public reporting their suspicions;
- media statements by spokesmen for terrorist groups or their sympathizers.

The quantity of material coming in is immense - and to some extent driven by market forces If someone is willing to pay for counter-terrorist intelligence then you can be sure that someone else is willing to supply it - manufacturing it first if necessary.

On this Material

The job of the intelligence officer is to identify those strands that are worth pursuing and then to pursue them until either they are resolved, or they start to look flakey and not worth pursuing, or there is nothing more that can usefully be done. It is a risk-management process. The number of potential leads that can be followed is virtually infinite. On the other hand covert investigation is extremely resource-intensive and impinges on the human rights of the subject. The threshold for such investigations is therefore high and the number of investigations necessarily limited. Consequently many potential leads have to be discounted. Decisions on which leads to pursue are vital, but are also complex and rich in judgement.

The British Foreign Secretary made a similar point in defending the Security Service's handling of the Bali bombing, by claiming that the Service receives 150 potential warning items each day. Globalized terrorism poses many challenges, but an ability to deal with extensive data of many different kinds seems a central criterion for an effective response.

So too is the need for secrecy. Much of the material is of covert intelligence provenance, foreign as well as national, and requires source protection; little of it is in the public domain. Follow-up investigations based on it need similar protection; good security is as necessary for counter-terrorist activity as for terrorism itself. Hence secrecy's pervasive effects.

These influence the character of intelligence as a whole. As an activity it has always been seen partly as covert collection - secretly acquiring other peoples' secrets - and partly as analyzing subjects and situations in wider 'all-source' contexts. Greg Treverton has characterized the two different aspects as 'intelligence-as-secrets' and 'intelligence-as-information', the latter making more use of open source material and including the more speculative, 'iffier' estimates and forecasts often most relevant to central decision-taking.[3] Views of intelligence have tended to emphasize either one feature or the other. In the Cold War most investment was in covert collection, and the collection of secrets predominated, but commentators for much of the 1990s argued that the future lay in analysis. More information was becoming openly available; covert collection would fill gaps, but the most important contribution would be wise analysis for top government. After the end of the Cold War, the present author argued that intelligence would become increasingly variegated, flexible and opportunistic. In terms of Britain's survival it is now less vital than during the Cold War, but

probably more useful.... British intelligence's national importance therefore needs to be judged mainly in rather general contexts: public assumptions about foreign policy and defence; long-standing expectations of intelligence as a strong card in government's hand; the links between intelligence and the transatlantic political relationship.[4]

On this view it was possible for a liberal to expect that intelligence would become rather less mysterious and 'special', and more like a normal information service such as government statistics; more open and unspectacular, and attracting less media curiosity and hype.

How overtaken by events this now seems! Already by the end of the 1990s the pendulum was swinging back some way towards the older view. Operations in the former Yugoslavia had demonstrated the continued need for secret collection, and for support for the use of armed force. Yet there still seemed to be no overarching threat; Western military interventions were still interventions by choice. 9/11 and subsequent terrorism have now radically altered the situation. As in the Cold War, intelligence is again targeted on a major threat from an intensely difficult target; but arguably the threat is now actual, not latent, and even more impenetrable than then. In the Cold War, intelligence was helping its governments to avoid war; now it is actively involved in one, saving lives and defending national security in the most literal sense. Whatever reservations there may be about describing Western reactions to 9/11 as 'war', the wartime metaphor fits intelligence's changed status rather well.

Of course it will continue to have its many other, different tasks. Much of it will still be on political or military subjects, or combinations of the two in the mixed 'pol-mil' assessments needed on so many modern situations; and sometimes on the world of trade, finance and economics. And the counter-terrorist role is itself nothing new; Irish terrorism was a top priority for Britain for thirty years. But the threat then was limited in scale and geography, and seems relatively small compared with the globalization and destructiveness of contemporary terrorism. Counter-terrorism's importance will now cause intelligence to be slewed overall some way towards its requirements and skills.

The result may be to influence policy and perceptions about intelligence more than has yet been appreciated. Governments' legislation after 9/11 may presage a permanent shift in the balances between security surveillance and individual rights. The long-running dilemma of democratic openness versus official reticence will be heavily influenced by counter-terrorism's need for secrecy. Intelligence's value for money may come to be judged less by its top-level policy inputs than by its 'sharp-end' counter-terrorist effectiveness: Dame Stella Rimington's claim in 1994 that the security forces in Northern Ireland were by then frustrating four out of every five planned terrorist attacks illustrates the cumulative but unspectacular significance of successful tactical pre-emptive warnings.[5] None of this reduces the need for understanding the adversary's mind and tackling other broad questions; yet the reality of counter-terrorism puts a special premium upon nitty-gritty analysis and smart operational use.

The effects of a re-evaluation of this kind may spread more widely in unexpected ways. Thus at an academic level the received doctrine about 'warning failures' probably needs rewriting to take account of the asymmetric warfare in which counter-terrorism is engaged. All this could be part of a general twenty-first century sea-change in thinking about intelligence as a whole.

This paper does not speculate further on the form this may take, but concentrates instead on one particular aspect. If the core of counter-terrorism is indeed tracing threads and weaving patterns out of many different kinds of evidence, then it is a 'natural' for the application of the latest in ICT (information and communications technology) to work horizontally across all the separate institutions holding relevant data. It therefore poses questions about the vertical institutional boundaries that give individual agencies proprietary control of their own information. How far then does counter-terrorism link with the information revolution in calling established intelligence structures into question?

Community Structure

The structures of the English-speaking intelligence communities have in fact been surprisingly static since they took their main forms just after the Second World War. Apart from the integration of the separate armed services' central intelligence staffs, Britain's current structure is much as it emerged in 1945. Since the creation of the CIA and NSA in 1947 and 1952, the US community has also been relatively conservative in its make-up, except for the new organizations needed for intelligence satellites and the imagery they produce. Perhaps Canada's creation of CSIS out of the RCMP was one of the more radical English-speaking reforms. All this relative stability has been in a period in which reorganization has been endemic in other public administration, and 'agile organization' has become a modern managerial watchword elsewhere.

Before 9/11 there was no shortage of American writing about the need for change. Much of it was about specific American weaknesses. The National Security Agency was said to be fossilized; the new National Imagery and Mapping Agency should never have been created in the first place; the Defense Intelligence Agency had never found its real *métier*; the CIA for some writers was too civilian, and thought it had been too oriented to military support since the Gulf War. At the apex of the structure the DCI was held to be ineffectual, without direct control of money and jobs.

To some extent, this reflected the American propensity to seek improvement in everything, but it also reflected a wider, radical strain in organizational thinking. Intelligence's structure of separate and powerful agencies was seen to encourage 'stovepiping', in which single-source intelligence is passed up to the top without sufficient all-source integration. Writers criticized the resulting marketing of single-source rather than all-source material, the inter-agency rivalry, and the pursuit of agency rather than community interests. The tone was strongly anti-bureaucratic. 'Bureaucracies are bad. Secret bureaucracies are worse.'[6] Intelligence's future was held to lay in the modern organizational doctrine of de-layering, market-based models, virtual communities and team approaches.

One suspects that stovepiping had become here a convenient whipping boy for every kind of shortcoming. Intelligence requires high reliability, and organizational divisions are needed to maintain varied kinds of special expertise and accountability. Intelligence cannot be just a free-for-all. There has to be a leading agency that takes main responsibility for analysis and inputs to policy in quickly-moving emergencies, as the Security Service does in the UK. (Part of the American problem is that over foreign preparations for attacks on the homeland, it is not clear whether the CIA or the FBI leads). The issue is not the existence of the stovepipes but their number, length and arrangements for junctions with others.[7]

Nonetheless the criticism cannot be dismissed. In the present writer's (admittedly distant) experience, American satellite imagery in the Cold War was a technical and professional miracle, but its handling in separate organizations with separate security regulations meant that it was difficult for anyone to integrate it properly with other technical collection. Intelligence developed an ever-increasing labyrinth of special classifications and compartments, designed explicitly to control information flows; justifiably so, in Cold War conditions, but with damage nevertheless to effectiveness.[8] After his experience in the senior American community, Treverton memorably commented that *community* describes precisely what it is not: it is somewhere between a fiction and an aspiration.[9]

This seems particularly relevant to counter-terrorism's need to cope with diverse information. American post-mortems after 9/11 have been surprisingly unfocused up to now, but stovepiping - particularly its effects on information exchanges between the CIA and the FBI - will remain a central theme for full-scale investigation. The writer's impression is that, in English-speaking intelligence communities, modern ICT is being harnessed quite effectively to create classified intelligence Web sites for agencies' 'published' reports (those issued as end-product to intelligence consumers and other agencies), but that it is still not envisaged that analysts following up terrorist traces will be able to trawl automatically through the *unpublished* material in each others' databases.

One simplistic answer would be to reorganize, starting by eliminating the traditional distinction between 'domestic' and 'foreign' intelligence. This might not have spectacular effects in Canada, but in Britain would mean amalgamating the Security Service and the Secret Intelligence Service (the SIS). In principle this amalgamation would fit the globalization that now makes distinctions between foreign and domestic targets increasingly artificial. Terrorists are located partly abroad and partly at home and move easily in the world of extensive foreign travel, worldwide communications and international finance. So some reorganization around global terrorism is not altogether out of the question. It is interesting to speculate whether Britain would have been wise to create a more interdisciplinary, target-driven counter-terrorist organization of some kind in 1969, presumably under Security Service direction, if it had known that Irish terrorism would be a principal national preoccupation for the next thirty years.

Yet reorganization as a solution is in some ways facile, in others too difficult. It ignores individual organizations' particular skills and institutional links, particularly with opposite numbers overseas. Treverton put it neatly: 'the capacities embedded in existing intelligence organizations are both powerful and hard to create, so caution is called for in demolishing them in favor of something new while we are yet so uncertain of the world we will confront'.[10] 9/11 has not outdated his caution. The private sector, with different traditions of organizational fluidity, might well reorganize, but can run greater risks than governments.

So it will be surprising if Britain ever goes for amalgamation. There is American talk of creating an analogue of the Security Service out of the FBI, but over the integration of home and overseas efforts it seems inconceivable that the CIA would ever again get a mandate for the domestic coverage it was accused of mounting before the mid-1970s. However much they are interleaved, domestic and foreign intelligence agencies in democracies are subject to very different legal and political restraints, and develop distinctive casts of mind as a result. Merging them hardly seems practicable or desirable.

If reorganization is not an answer, correctives to stovepiping lie in ways of softening inter-agency boundaries and enabling ICT to develop 'virtual communities' across different organizations. Cross-postings between agencies, inter-agency training and similar initiatives have an important part to play in building up a greater 'community consciousness'. Intelligence may have something to learn here from the armed services' successes in developing operational 'jointery' while keeping their separate identities. A writer on public administration has opined that getting agencies to work together is a matter of behaviour and process, not structure; collaboration is a long-term process that turns on 'creating a climate of trust and joint problem-solving' that produces what he labels an 'Interagency Collaborative Capacity'.[11] If true of all government, this applies particularly to intelligence, where secrecy breeds an intense sense of belonging, but to a single agency and not a community. Intelligence literature emphasizes the need to be close to policy-makers; yet single-source agencies' highest priority in counter-terrorism is actually to be close to their all-source intelligence colleagues who work the problem as a whole.

This points to the importance of fruitful single-source/all-source relationships. The different responsibilities of the two have to be recognized: one as the expert on particular kinds of collection and exploitation, the other as government's all-round authority on a subject. Military intelligence doctrine is emphatic in differentiating between the two, and the present writer has written similarly that, through it, 'a valuable Western principle has evolved - by accident, not conscious design - that those collecting and processing information should not normally have final responsibility for evaluating it'.[12] Yet the institutional boundary impedes what intellectually is really an all-embracing search for truth, ideally a *jeu sans frontières* (a title given to the Eurovision Song Contest). 'Despite the value of the single- source/all-source distinction, it is still intellectually artificial to chop into two parts what in reality is a continuous search from truth. There are no pure, objective 'facts' delivered to the all-source analyst's front door. All-source analysis needs some ability to reach back into Sigint, and vice versa.'[13]

ICT now has the potential to make this approach to truth-seeking more of a reality, with data as a common asset which virtual communities can access freely. In one sense it is a rather obvious *desideratum*; some may claim that it is not far from what happens now, particularly when people are on good terms and have the stimulus of the terrorist threat. In another sense it is a revolutionary doctrine, wreaking havoc with well-established ideas of security protection and specialized agency skills and responsibilities. Despite its particular relevance to counter-terrorism, applying ICT in this way will be much harder in practice than it sounds. Determined leadership from the centre will be needed to reduce inter-institutional boundaries without throwing source protection overboard. But, if so, the question then arises: in intelligence, who leads?

Who Leads?

The British Joint Intelligence Committee (the JIC) evolved in the Second World War with two principal roles joined together by historical accident: directing wartime intelligence, mainly by agreement between the three armed services, and producing agreed intelligence assessments for those running the war. It has been quite widely imitated. Most English-speaking countries recognize that committees have a place in producing top-level estimates, though they vary in the precise roles attached to them. Committees are also needed to manage intelligence, though almost everywhere they are complemented by central authority somewhere in the system. There has been a general tendency - less in Britain than elsewhere - for the machineries of community assessment and management to separate. Both are bound to evolve further. How will counter-terrorism affect their evolution?

One effect may apply to both. The importance of counter-terrorism has joined with the sheer pace of modern government - the constant need for immediate action and reaction - to focus attention on the question 'Who's in charge?', put by Churchill in 1940 about the British system. In Britain as elsewhere there is no clearer answer now than then. As intelligence becomes more important and decisions more pressing, governments and media will become increasingly dissatisfied with answers in terms of committees and communities, and will call for an identifiable national Chief Intelligence Officer. In the American system the post already exists in the person of the DCI, but it has long been argued that he lacks managerial teeth; the problem is devising practical ways of providing them. In Britain the JIC Chairman is a titular head of the community, yet there has always been a deep reluctance to accord the occupant a proconsular role in an innately collegial system.

So in both systems top posts exist, but their impact is unusually dependent on personal qualities plus backing from above. Enhanced power for the DCI post figured among the recently stated presidential objectives, though there is no indication how this is to be provided. In Britain the position is clearer. As part of reorganization at the centre, Sir David Omand has recently joined what is almost a dyarchy at the top of the Cabinet Office, in which he has responsibility for coordinating all intelligence and security matters including counter-terrorism. This does not solve the problem of ministerial support

and responsibility in a Westminster-style system, but certainly strengthens the centre's clout at official level. Committees have their place, but terrorism's threats are likely to reinforce the trend in government towards identifying personal accountability.

So in both systems, and perhaps in other English-speaking ones as well, the effects of counter-terrorism may turn out to lie not in changing formal intelligence structures, but in the *de facto* authority of the top posts at the centre. In America, the position of the present DCI, as a Clinton appointee continuing under the Bush Administration, may be a precedent for greater continuity and authority. In the UK, all JIC Chairmen before 2001 came from the Foreign Office, usually in combination with other duties; and although intelligence was well-served by the high calibre of the post's occupants, the fact of being high fliers tended to make them also birds of passage. Since just before 9/11 the post has been occupied for the first time by a full-time intelligence professional likely to stay there for some time, and events since then have underlined the requirements originally stated in 1947 that the Chairman should have 'an assured position, adequate time and sufficient supporting staff' to provide 'the added authority that is needed to give more forcefulness and influence to our intelligence organization as a whole'.[14]

So perhaps counter-terrorism everywhere will re-emphasize intelligence leadership, and with it the need for continuity in post and adequate preparation in previous careers. Possibly a national Head of Intelligence role may eventually become recognized and professionalized in the same way as governments' heads of other specialized disciplines, with consequent reduction in agencies' autonomy. This may pose its own problems, but the post-9/11 climate at least gives governments scope for giving the community this option. But in a century of rapid change, what community will this actually be?

What Community?

Intelligence is a broad church; there is no formal definition of the subjects it should not tackle. The British JIC has a mandate to assess almost anything, and expands *ad hoc* to include representatives of other departments when dealing with matters outside its normal sphere. But in practice its main impact is usually when it deals with the world of threats, warning, violence, international disorder and war. Washington has tended to take a rather broader view, for example in the production of CIA's futurologies of world trends. Yet at least until the end of the Cold War there was a general assumption in English-speaking countries that intelligence was most needed on 'national security' matters of one kind or another, more carefully defined in domestic contexts than foreign ones.

This underwent some change in the decade after 1990. There was discussion of economic intelligence as a growth area, though in the end it remained much as before. More innovative were the developing intelligence connections with law enforcement authorities, mainly police, immigration and customs. These were not new, but were expanded in both the UK and US to develop intelligence agencies' collection on drug trafficking, money laundering and other organized crime, especially when international. Drugs became a major CIA commitment and a JIC First Priority collection

requirement, and the JIC produced papers on the subject. There were media reports that Britain's Security Service had been tasked with arcane aspects of police corruption, and the SIS with tracking the organizers of illegal immigration, which also became a matter for JIC assessment. Even military intelligence was sometimes targeted on crime, as when military forces for peace support in Bosnia and Kosovo needed intelligence on the local and international mafia.

At the same time 'intelligence' itself developed as a new specialization within law enforcement institutions themselves, and in Britain showed signs of developing as a nascent intelligence community on its own account, led and coordinated by the new National Criminal Intelligence Service (NCIS). At least in the UK, the favoured sound-bite for greater police effectiveness has become 'intelligence-led policing'. Joint interests with the 'old' intelligence community are recognized by the attendance of the NCIS at JIC meetings. Both the UK and US established intelligence exchanges on international crime with the KGB's successors in modern Russia. So even before 9/11 there was scope for speculation about the future boundaries between the 'new' and 'old' intelligence, and the possibility that the two might in the long term merge, particularly as sophisticated crime became more transnational, especially in Europe and presumably also in the Americas.

Counter-terrorism now gives additional force to the speculation. It makes close cooperation between the two sets of institutions particularly important; law enforcement is both a major contributor of intelligence on terrorism and a prime customer for it. In Britain the study of terrorist funding is performed principally by the NCIS; the National Counter Terrorism and Security Office is manned jointly by police and the Security Service; and the Police International Counter Terrorist Unit includes Security Service representatives. In the US the need for better cooperation of this kind was another theme of the Presidential address already quoted. Terrorists are usually not criminals in a conventional sense, but their infrastructure is very likely to involve them in forms of criminality and law evasion.

Large issues of principle arise, of course, over any governmental integration of personal information about its citizens, and its use for multiple purposes. There is libertarian anxiety about the official American research program of Total Information Awareness, which envisages tracing terrorists by matching *inter alia* passport and visa applications, criminal, education and housing records, travel and transportation information, as well as personal identity data like fingerprints and iris scans. Even the present British government's non-security objective of using ICT to link government's separate services to the citizen in 'joined up government' has aroused similar fears of Orwell's 1984. In institutional terms, however, the needs of counter-terrorism might nevertheless seem to point towards expanding the traditional intelligence communities with increased law enforcement responsibilities and representation.

Yet even in an information revolution there are substantial objections to radical changes of that kind. The basic difference remains between law enforcement's main concern with 'normal' crime for financial gain, and terrorism's use of violence for political ends. In Britain it would be surprising

if the JIC were expanded to include the NCIS and other law enforcement organs as full members, and took on substantial segments of crime among its permanent responsibilities; and it would on the whole be undesirable as well as unlikely. On the other hand the American lesson about the need to pool foreign intelligence with domestic data seems so compelling that it will be surprising if some US changes do not follow the creation of the new Department of Homeland Security. Perhaps all that can be said is that counter-terrorism accentuates the increased interdependence of the (old) intelligence community and its (new) law enforcement analogue. Intelligence as traditionally understood has always had some fuzzy boundaries, and law enforcement intelligence and its involvement in counter-terrorism is adding another.

How International?

Quite apart from its involvement in the overseas as well as domestic dimensions of law enforcement, foreign collaboration had become increasingly prominent in intelligence's normal activities before 9/11. Foreign liaisons are of course nothing new. They were an important feature of the West's Cold War alliances, but further extended in the 1990s. International terrorism was already a major target. Governments' actions involving military power were also becoming increasingly multilateral, as in the former Yugoslavia, and these were themselves becoming increasingly intelligence-led. The same applied to the growing international attempts to monitor and restrain WMD development and other threats. A considerable growth of intelligence-sharing followed. Before 9/11, CIA already had relationships with 400 foreign intelligence and security organizations, and at that time the Russian FSB (the ex-KGB equivalent of CSIS) was similarly claiming to have 'around 80 missions representing the special services of 56 countries' working permanently in Moscow, and formal agreements with '40 foreign partners in 33 countries'.[15] Up to UNSCOM's withdrawal in 1998, up to twenty nations are said to have passed information to it on Iraqi sanctions-busting and weapons development.

But 9/11 has given a great boost to this 'internationalization'. It brought home to the US that, despite being an intelligence superpower, it cannot meet all its counter-terrorist requirements itself. Almost every nation is able to supply some unique intelligence on global terrorism, from its local records and local human and technical sources; from local telephone tapping, for example. Security Council Resolution 1373 immediately after 9/11 explicitly mandated such exchanges, though in UN style these were still described as 'information'. America developed a set of new counter-terrorist relationships, and Britain followed suit, notably in the Blair-Putin announcement in December 2001 of new Anglo-Russian machinery for the purpose. A year later the presidential message of September 2002 formally confirmed the American objective of coordinating closely with allies for common assessment of the most dangerous threats. The Security Service, necessarily the most domestically oriented British agency, by then was claiming to have over a hundred overseas links.[16]

The move to more cooperation has not always been consistent. US policies vary between cultivating international support and going it alone, and no doubt influence the climate in intelligence as in everything else. Nevertheless the increase in inter-governmental intelligence collaboration since 9/11,

sometimes between unlikely allies, has been striking in what, despite foreign liaisons, had formerly been instinctively regarded as an essentially separate, reclusive national activity, deeply rooted in secrecy and national interests: waging a special zero-sum information contest between states, some way removed from the main fabric of international relationships, a matter for special people in special compartments. By contrast, intelligence collaboration is now regularly in the news, almost as often as the older elements of international relationships.

Cooperation may therefore provide another element in a sea-change in thinking about intelligence as a whole. 9/11 re-emphasized the covert aspects and need for secrecy. But it must also have intensified the shift already apparent in the 1990s away from governments' targeting of what the Victorians called 'civilized' states, and towards a concentration on non-states (including terrorist organizations), problem states and situations, and rogue states outside the international pale, particularly those supporting and harbouring terrorism. Al Qaida, Iraq and North Korea typify the new category, and their importance must mean less coverage of 'normal' states as an adjunct to regular diplomacy and negotiation; the ten per cent which a distinguished British diplomat once estimated as the addition that covert intelligence added to regular diplomatic reporting.

From this comes the possibility of a new paradigm for intelligence. In the international system of (normal) states, it is moving to becoming, not a zero-sum contest, but a cooperative activity between them, directed against common threats and common concerns. Even major policy disagreements - as at the time of writing over the action to be taken over Saddam Hussein's evasion of UN inspection - are based on shared (or partially shared) evidence; intelligence has become the material of worldwide inter-governmental and public discourse. The paradigm of cooperative intelligence activity and interpretation was implicit in the developments of the 1990s, but with 9/11 and subsequent events it can now be articulated.

Possible results of the new paradigm have been discussed elsewhere[17] in terms of international intelligence collection and the development of multilateral and international analysis. There are already some precedents for UN-controlled collection — blue-helmeted tactical units in the Congo and operations in the former Yugoslavia; the American U-2 sorties over Iraq controlled by UNSCOM; the similar collection for UNMOVIC. But this is unlikely to be a main line of development. Most collection will remain a national activity, but with more formal international pooling and discussion of results. The UK-US-Commonwealth community has its long-standing arrangements for joint participation in the production of intelligence estimates such as those of the JIC, and there is no intrinsic reason why the NATO Council should not have similar machinery for intelligence drafted by an international intelligence staff. There is equally no reason why the Security Council should not have something similar at its disposal, though there it would need to be labelled 'assessment' and not 'intelligence'. UNMOVIC is reported today as having convened a meeting of 'missile experts' from six countries to assess the evidence on Iraqi missiles along with its own analysis staff. What is this but a *de facto* international assessment staff?

Developing cooperative intelligence and formal intelligence machinery of this kind may seem pie-in-the-sky for what is still closely guarded national activity. It assumes that states will actually practice greater restraint in intrusive collection against each other, recognizing that a kind of 'intelligence arms control' would assist cooperation and free resources for use against the new targets; that intelligence is not automatically associated with covert action; that governments worldwide will come to expect some professional truthfulness from it, rather than view it as inseparable from policy. The KGB's official definition of intelligence-gathering was as 'a specific form of political struggle used by the intelligence agencies of a state to help it to fulfil its internal and external functions'.[18] Stripped of its ideology this is still the widely held international view. Few governments or publics believe that intelligence is not just a currency for exploitation for policy or power.

Yet nations and their leaders can change their working assumptions quite radically over time. In intelligence itself, National Technical Means of information collection (the euphemism for Sigint and imagery) received a totally unforeseeable legitimacy through US-Soviet strategic arms control in the Cold War and subsequent international agreements.[19] More broadly, war between states before the eighteenth century Enlightenment 'remained an almost automatic activity, part of the natural order of things.... If anyone could be said to have invented peace as more than a mere pious aspiration, it was Kant.'[20] In the nineteenth century the Red Cross owed its development to a private initiative which caught on and moved governments;[21] and the Hague Conference of 1899 and its contributions to the laws of war originated in an unexpected initiative from the Tsar, possibly from reading a book on future war.[22] Views of military power itself are now undergoing a similar transformation, as in the British writer's view of democracy's professional soldiers as international society's check upon violence; 'those honourable warriors who administer force in the cause of peace.'[23] *Mutatis mutandis*, the terrorist threat opens up a similar view of intelligence. So just as 9/11 leads governments to lower information boundaries within their own national systems to improve inter-agency cooperation, so also it points to a more cooperative view of intelligence internationally.

Conclusion

11 September 2001 has made counter-terrorism intelligence's overarching priority. It requires a near-wartime intensity to meet it, will not be transitory, and will be a major influence on intelligence's overall character. Intelligence is simultaneously part of the revolution in information and communications technology (ICT), a revolution that is peculiarly suited to meet counter-terrorism's distinctive need for detecting connections in large swathes of many different kinds of data, but one that also changes organizations, relationships and communities in quite radical ways. Hence applying it to full effect in counter-terrorism calls into question intelligence's long-standing structures and boundaries, and the single-agency 'stovepiping'that these encourage.

Thus reorganization for international terrorism by merging all related 'foreign' and 'security' intelligence into one ICT-driven agency might appear logical; but it would in fact be facile. The antidote to stovepiping will instead be in cultural adaptations of varying kinds to promote the greater

'community consciousness' needed to develop ICT systems spanning across inter-agency boundaries. Promoting this consciousness requires central intelligence leadership. So too does the need to cope with the sheer pace of modern government and its demands on intelligence. Committees still have their place, but governments will increasingly expect to have their Chief Intelligence Officers, with full responsibility for their national intelligence communities.

These communities will themselves change in other ways. Counter-terrorism will emphasize the need for increased connections with law enforcement and its new law enforcement intelligence 'communities'. In another dimension they will become increasingly international in the services they provide. They will remain national institutions, but will be seen increasingly as supporting inter-state cooperation for shared objectives, primarily but not exclusively counter-terrorism: in a sense, states' defence against their non-state enemies. They will remain deeply influenced by counter-terrorism's need for secrecy, yet will at the same time adapt to the need for more cross-boundary working - within their own communities; with law enforcement organs and others involved in counter-terrorism; with foreign opposite numbers; and with specialist assessment machinery at NATO, the UN and other regional and international levels.

End Notes

1. Bruce D.Berkowitz and Allen E.Goodman, Best Truth: Intelligence in the Information Age (New Haven and London: Yale University Press, 2000), p.98.

2. Published in Security Monitor (RUSI London) first issue, 2002. Quotations from this article.

3. Gregory F.Treverton, Reshaping National Intelligence for an Age of Information (Cambridge University Press, 2001), passim.

4. Author, British Intelligence towards the Millennium (London: Centre for Defence Studies, pp.64-65.

5. S. Rimington, Richard Dimbleby Lecture Security and Democracy (London: BBC Educational Developments, 1994), p.9

6. Address by Robert Steele, St Antony's College Oxford, 12 June 2002.

7. I am indebted for these balancing comments to the late Colonel Kevin Cunningham, US Army War College.

8. The present American Defense Secretary is said to have complained that a recent briefing on national missile defence had been chaotic since, because of compartmentation, no analyst could present the total picture.

9. Treverton, p.xiii.

10. Treverton, p.249.

11. E.Bardach, Getting Agencies to Work Together: the Practice and Theory of Managerial Craftsmanship (Washington DC: Brookings Institute), quoted by Wayne Parsons, 'Modernising Policy-Making for the Twenty-First Century: the Professional Model', Public Policy and Administration vol.16 no.10 (autumn 2001).

12. Author, Intelligence Power in Peace and War (Cambridge: Cambridge University Press, 1996), p.112.

13. Author, Intelligence Services in the Information Age (London: Cass, 2001), p.193.

14. Evill report in 1947 on the JIC, quoted in Intelligence Services in the Information Age, p.114.

15. Article by FSB Director N.Patrushev, Russian National Information Service 20 December 2001.

16. MI5: The Security Service (offical publication, fourth edition, available 2002), p.26.

17. Author's '11 September: Legitimizing Intelligence?', International Relations vol.16 no.2 (August 2002).

18. Vasiliy Mitrokhin, KGB Lexicon: The Soviet Intelligence Officer's Handbook (London: Cass, 2002), p.200.

19. History outlined in Intelligence Power in Peace and War, pp.159-62.

20. Quotations from M.Howard, The Invention of Peace: Reflections on War and International Order (London: Profile Books, 2000), pp.13 and 31.

21. Pam Brown, Henry Dunant: The Founder of the Red Cross (Watford: Exley, 1988).

22. G.Best, 'Peace Conferences and the Century of Total War: The 1899 Hague Conference and What Came Afte',International Affairs, vol.75 no.3 (July 1999), p.622.

23. Concluding words in J.Keegan, War and Our World (London: Hutchinson, 1998) (Reith Lectures 1998), p.74.

Michael Herman (MHe24@aol.com) was in British government service from 1952 to 1987. He is now associated with St Antony's College Oxford and Aberystwyth University. He has published Intelligence Power in Peace and War (1996) and Intelligence Services in the Information Age (2001).

Commentary is a regular publication of the Research, Analysis and Production Branch of CSIS. Inquiries regarding submissions may be made to the Director General of the Research, Analysis and Production Branch at the following address: Box 9732, Stn. "T", Ottawa, Ont., K1G 4G4, or by fax at (613) 842-1312. Consult our World Wide Web site on the Internet for back issues of *Commentary*: http://www.csis-scrs.gc.ca

ISSN 1192-277X
Catalogue JS73-1/83

Non classifié
Été 2003
N° 83

Service canadien du renseignement de sécurité

Commentaire

Le renseignement après le 11 septembre : un point de vue britannique

Michael Herman

Commentaire exprime les opinions des auteurs et ne suppose pas que le SCRS y souscrit ou en endosse l'authenticité.

Introduction

Si la déclaration de guerre au terrorisme faite par le président Bush à la suite des attentats du 11 septembre 2001 n'a pas été bien accueillie partout, on ne peut plus douter aujourd'hui qu'Al Qaida est en guerre contre les États-Unis – une première attaque avait été lancée contre le World Trade Center en 1993 – et que les autres pays de l'« Ouest capitaliste » (peu importe la définition qu'on donne à celui-ci) doivent désormais vivre sous la menace en raison de leur « alliance » avec les Américains. Au moment où nous écrivons ces lignes (hiver 2002-2003), le gouvernement britannique fait grand cas d'une éventuelle attaque terroriste à l'arme chimique, biologique ou radiologique et met en garde la population : il est impossible de garantir une sécurité sans faille, totale. Présumant que de tels avertissements reposent sur des éléments concrets, nous vivons dans un climat dominé par une sérieuse menace, situation qui n'aura rien de passager.

On peut donc estimer que le renseignement va de soi dans le contexte de la lutte contre le terrorisme. La place qu'il occupe dans la pensée américaine a été mise en évidence dans la *National Security Strategy*, le 20 septembre 2002 : le président Bush y a fait 18 fois référence en parlant des principaux atouts nationaux – le renseignement n'est surpassé que par les moyens militaires (24 allusions) et devance largement la diplomatie, citée sept fois. À l'exemple des États-Unis, la plupart des pays occidentaux ont augmenté les crédits consacrés à leurs services de renseignements et assoupli les restrictions légales à leurs activités. Partout, le renseignement a la cote.

Notons qu'il ne s'agissait pas, à proprement parler, d'un revirement complet de la situation. D'accord, les services de renseignements avaient perdu de leur importance avec la fin de la guerre froide (c'était là un des dividendes de la paix), mais déjà avant le 11 septembre, les budgets qu'on leur réservait étaient à la hausse non seulement parce qu'il fallait faire face au terrorisme, mais également parce qu'on devait tenir compte des impératifs des années 90 : participation aux opérations internationales axées sur le maintien de la paix ou l'aide humanitaire, collecte de données sur la prolifération des armes de destruction massive, sur le non-respect des sanctions, sur le trafic des stupéfiants et sur les nouveaux défis de la décennie. Les gouvernements cherchaient déjà à s'adapter à ce qui semblait un monde de plus en plus instable, de même qu'à la révolution touchant l'information accessible et à leur capacité de recueillir et de traiter cette dernière. Les satellites de renseignement avaient cessé d'être l'apanage des superpuissances et, déjà, toute une gamme de puissances secondaires en exploitaient ou prévoyaient le faire. Le renseignement dans son ensemble gagnait en légitimité au sein de l'État; on n'avait plus à en nier l'existence.

Les événements du 11 septembre 2001 ont renforcé cette tendance de façon spectaculaire, confirmant la place qu'occupe le renseignement dans la panoplie des éléments essentiels d'un pouvoir national discret (ou à moitié discret). Toutes les nations, sauf les plus modestes, vont bientôt prendre certaines mesures à cet égard – si ce n'est déjà fait. Les attentats ont également mis en lumière le rôle joué par l'antiterrorisme dans le tableau global du renseignement : dorénavant, on peut le tenir pour une catégorie distincte et importante des services de renseignement, semblable aux sous-ensembles politique, militaire et économique qui existaient antérieurement et comprenant une grande partie de

ce qu'on appelait, jusqu'alors, le « renseignement de sécurité ». Nul doute que ce volet entrera en concurrence avec d'autres impératifs – à l'heure actuelle, par exemple, la recherche de preuves tangibles de l'existence d'armes de destruction massive mises au point par Saddam Hussein revêt une priorité semblable pour les États-Unis –, mais il semble néanmoins exercer une influence dominante et durable sur le milieu du renseignement.

Quoi qu'il en soit, le renseignement est appelé à changer de façon radicale dans le cadre de la révolution de l'information, dont il fait d'ailleurs partie. Comme le faisaient remarquer deux écrivains américains avant le 11 septembre, « si les services de renseignements veulent conserver leur efficacité, les milieux qui les composent devront se prêter à des changements d'une ampleur telle que, cette étape franchie, on aura peine à reconnaître l'organisation créée il y a cinquante ans »[1] (trad. libre). Mais la place prépondérante qu'occupe l'antiterrorisme, pratiquement sur le pied de guerre pour longtemps, imposera au processus un rythme particulier.

On s'interroge, dans ce document, sur l'avenir du renseignement et sur les défis qui lui sont associés. L'auteur, britannique, y fait part de son opinion personnelle à la lumière de la situation prévalant dans son pays et des récentes proclamations américaines. Il s'attardera quelque peu aux services de renseignements occidentaux dans leur ensemble, et peut-être même plus en détail.

Antiterrorisme et nature du renseignement

Le renseignement sur le terrorisme – ou, si l'on veut, l'antiterrorisme – repose d'abord sur le repérage et le pistage de *personnes* ainsi que sur la découverte de leurs projets et activités. Il s'intéresse aux individus plutôt qu'aux choses, ce qui contraste avec le renseignement de nature militaire, qui met l'accent sur le *matériel* militaire et sur l'ordre de bataille des unités structurées. Son but : le dépistage plutôt que l'analyse de situations d'ensemble, démarche centrale de nombre d'autres services de renseignements – on pense, par exemple, à la connaissance de la situation du champ de bataille rendue possible par la puissance des techniques modernes de collecte de données. Voilà pourquoi, avant comme après le 11 septembre, le débat ayant entouré l'antiterrorisme s'est articulé pour une grande part autour de la nécessité d'améliorer au premier chef ce qu'il est convenu d'appeler le renseignement humain (HUMINT).

Pareille conjoncture peut avoir laissé transparaître des traces de naïveté ou avoir donné lieu à la quête d'une panacée. De bonnes sources humaines de renseignements sur le terrorisme valent leur pesant d'or. Les succès qu'ont connus les forces britanniques dans leur lutte contre l'Armée républicaine irlandaise (IRA) leur ont été largement tributaires. En réalité, les observateurs américains ont peut-être raison lorsqu'ils soutiennent que les critiques constantes du Congrès et des médias, conjuguées à l'absence de soutien de la direction, ont démoralisé les responsables de la direction des opérations de la CIA. Mais il serait pour le moins chimérique de placer trop d'espoir même dans un effort accru de l'HUMINT lorsque les cibles/objectifs sont, à ce point, obnubilés par la sécurité.

Le défi le plus important et le plus singulier de l'antiterrorisme ne se situe peut-être pas dans un type particulier de collecte de données, mais plutôt dans la recherche de liens entre des preuves nombreuses et de divers types. Récemment, un membre de l'International Counter Terrorist Branch du British Security Service (BSS) a rédigé un document pertinent[2], dans lequel il affirmait que l'antiterrorisme ne consiste ni en une partie d'échecs contre un seul ennemi ni en la réalisation d'un puzzle, à moins qu'on n'accepte d'avance que l'image à reproduire soit fragmentaire et évanescente et que nombre des pièces contenues dans la boîte soient inutiles. En quête d'une piste, il opte pour la métaphore des fils conducteurs repérables et des motifs tissés. Les matériaux de base eux-mêmes sont bigarrés et d'une diversité considérable. On pense, entre autres choses :

- aux renseignements secrets glanés au fil des communications (interceptées) de terroristes connus;
- aux renseignements secrets portant sur ceux qui, au pays ou à l'étranger, sont réputés avoir déjà été parties prenantes à des activités de soutien au terrorisme;
- aux rapports d'organismes de sécurité étrangers – rapports parfois teintés d'une saveur politique et d'une qualité éminemment inégale – faisant état de projets, concrets ou potentiels, d'attaques terroristes;
- aux rapports des services de police signalant, par exemple, des allées et venues suspectes dans des ports;
- aux allégations émanant de particuliers qui, d'eux-mêmes, viennent avouer posséder des renseignements de première main concernant des projets terroristes;
- aux appels de simples citoyens soucieux de déballer leurs soupçons;
- aux déclarations, rapportées par les médias, des porte-parole de groupes terroristes ou de leurs sympathisants.

Les éléments de renseignement affluent en quantité incroyable et le tout est, dans une certaine mesure, assujetti aux forces du marché : si l'on est prêt à payer pour obtenir des renseignements antiterroristes, il se trouvera assurément quelqu'un qui sera disposé à en fournir – quitte, au besoin, à les fabriquer de toutes pièces.

Face à cet afflux de données

L'agent de renseignements a pour tâche de cerner les fils conducteurs qui méritent une investigation plus poussée et de se lancer dans celle-ci jusqu'à ce qu'il connaisse le fin mot de l'histoire; il peut procéder en ordre inverse et commencer par éliminer les renseignements qui ont l'air trop loufoques et qui ne valent pas le coup ou qu'on a exploité jusqu'à la trame. Il s'agit-là d'un processus de gestion du risque. Virtuellement, le nombre de pistes est infini. D'un autre côté, une enquête secrète monopolise énormément de ressources et empiète sur les droits de la personne qui en fait l'objet. Voilà pourquoi le seuil à respecter pour lancer de telles enquêtes est élevé (facteur qui explique leur nombre nécessairement limité) et pourquoi beaucoup de fils conducteurs possibles sont écartés. Les décisions à cet égard – quelles pistes suivre ou non – sont vitales et complexes; elles supposent un discernement à toute épreuve.

Le secrétaire au Foreign Office a fait ressortir un aspect semblable, lorsqu'il a justifié la façon dont le BSS avait traité l'affaire de l'attentat à la bombe à Bali, en soutenant que les responsables reçoivent 150 avertissements chaque jour. Le terrorisme mondial suppose de nombreux défis et la capacité de traiter des données détaillées de divers types semble constituer un critère incontournable d'une réaction efficace.

Entre aussi en ligne de compte la nécessité du secret. Peu des éléments traités sont du domaine public : pour une grande part, ils proviennent de sources secrètes, au pays ou à l'étranger, qui doivent être protégées; s'ils donnent lieu à des enquêtes complémentaires, celles-ci doivent également être protégées. Une bonne sécurité est aussi essentielle aux activités antiterroristes qu'elle l'est aux activités terroristes elles-mêmes. D'où l'omniprésence du secret.

Pareille réalité influe sur la nature du renseignement dans son ensemble, activité qu'on a toujours associée, en partie, à une démarche secrète de collecte d'information – l'acquisition clandestine de secrets – et, en partie, à l'analyse de questions et de conjonctures dans des contextes plus généraux, en recoupant des données de toutes sources. Greg Treverton a dépeint les deux différents aspects de cette réalité : les renseignements assimilés aux secrets et les renseignements assimilés à l'information, ce dernier volet puisant davantage aux sources ouvertes et incluant des appréciations et prévisions d'ordre plus conjectural – qui, souvent, se prêtent davantage aux prises de décisions centralisées[3]. Les services de renseignements ont eu tendance à mettre l'accent soit sur l'une, soit sur l'autre de ces caractéristiques. Pendant la guerre froide, on investissait surtout dans la collecte secrète de renseignements, et la collecte de secrets prédominait; mais pendant la plus grande partie des années 90, les observateurs affirmaient que l'avenir, dans ce domaine, passait par l'analyse. Il y avait de plus en plus d'information ouvertement accessible et, si des activités secrètes de collecte pouvaient combler les lacunes, la fonction la plus significative des services concernés résidait dans une analyse avertie à l'intention des hauts responsables du gouvernement. Après la fin de la guerre froide, l'auteur soutenait que le renseignement deviendrait de plus en plus hétéroclite, souple et opportuniste. Le renseignement est désormais moins vital à la survie de la Grande-Bretagne qu'il ne l'était durant la guerre froide, mais il est sans doute plus utile. (...) L'importance nationale du renseignement britannique doit dès lors être estimée surtout dans des contextes plus généraux : hypothèses publiques relatives à la politique étrangère et à la défense; attentes à long terme des services de renseignements (atout dans le jeu du gouvernement); liens entre le renseignement et les relations politiques transatlantiques[4]. (trad. libre).

À partir de là, un esprit libéral aurait décemment pu s'attendre à ce que le renseignement perde de son auréole de mystère et d'extraordinaire et s'aligne sur les services d'information plus « normaux » – les statistiques gouvernementales, par exemple –, quelque chose de moins spectaculaire, suscitant moins la curiosité des journalistes et se prêtant moins au battage mené par les médias.

Pareille vision a été drôlement dépassée par les événements! Déjà, à la fin des années 90, le balancier redonnait quelque vigueur à l'ancienne conception des choses. Les opérations dans l'ex-Yougoslavie ont fait ressortir la nécessité permanente des activités secrètes de collecte et le besoin d'étayer le

recours aux forces armées. Pourtant, on ne semblait pas, à l'époque, faire face à une menace d'envergure et les interventions militaires des pays occidentaux étaient encore une question de choix. Le 11 septembre et les menées terroristes ultérieures ont modifié du tout au tout la donne. Comme pendant la guerre froide, les services de renseignements s'intéressent surtout à une menace majeure émanant d'une cible étonnamment difficile à cerner; mais tout porte à croire que la menace est désormais réelle et non plus latente et qu'elle est encore plus impénétrable qu'elle ne l'était alors. Pendant la guerre froide, les services de renseignements aidaient leurs gouvernements respectifs à éviter la guerre. Aujourd'hui, ils prennent activement part à une guerre, s'efforçant de sauver des vies et de défendre la sécurité nationale au sens le plus strict du terme. Quelles que soient les réserves soulevées lorsqu'on fait allusion à la guerre pour décrire les réactions occidentales aux attaques terroristes du 11 septembre, la métaphore du « temps de guerre » se prête assez bien aux nouvelles conditions dans lesquelles évoluent les services de renseignements.

Ceux-ci continueront, évidemment, à remplir diverses autres fonctions qui, dans bien des cas, relèveront toujours des domaines politique ou militaire – ou des deux à la fois, dans les appréciations composites politico-militaire qui s'imposent dans tant et tant de situations actuelles –, voire, parfois, du monde des affaires, des finances et de l'économie. En soi, le rôle antiterroriste qu'ils jouent n'a rien de neuf : le terrorisme irlandais a été la principale priorité des Britanniques pendant trente ans. Mais la menace était, alors, limitée tant par son ampleur que par la zone géographique visée; il semble même qu'elle ait été relativement faible si on la compare à celle qui émane du terrorisme contemporain, à la capacité destructrice *mondialisante*.

L'antiterrorisme gagnant en importance, les services de renseignements seront peut-être obligés de se réorienter, d'une manière ou d'une autre, en fonction de ses exigences et ses besoins. Il peut en résulter une incidence accrue sur les politiques et sur les perceptions relatives au renseignement. Les lois adoptées par les gouvernements après le 11 septembre peuvent laisser présager un virage permanent au regard de l'équilibre entre la surveillance à des fins de sécurité et les droits individuels. Le dilemme de longue date mettant en opposition transparence démocratique et réticence officielle sera grandement influencé par le besoin de secret entourant la lutte antiterroriste. Peut-être associera-t-on moins l'optimisation des ressources, dans ce domaine, à l'appui aux instances politiques suprêmes qu'à l'efficacité pointue en matière d'antiterrorisme. La déclaration de dame Stella Rimington, en 1994, qui affirmait que les forces de sécurité en Irlande du Nord contrecarraient quatre projets d'attaque terroriste sur cinq, illustre bien la signification cumulative mais peu spectaculaire d'avertissements tactiques préventifs fructueux[5]. Rien, dans tout ceci, ne vient réduire l'obligation de pénétrer l'esprit de l'ennemi et d'aborder d'autres grandes questions. En fait, la réalité de l'antiterrorisme suppose que l'on porte une attention spéciale à l'analyse de fond et à une exploitation réfléchie des données.

Pareille réévaluation peut faire des vagues dans des directions inattendues. Au niveau théorique, par exemple, la doctrine consacrée concernant les « avertissements lettre morte » devra sans doute être repensée pour tenir compte de la nature asymétrique de la lutte au terrorisme. Tout ceci pourrait bien faire partie de l'évolution générale profonde qui, au XXI[e] siècle, touchera le concept même du renseignement dans son ensemble.

On ne s'interroge pas ici sur la forme que ce dernier pourrait prendre. On s'intéresse plutôt à un aspect en particulier. Si, essentiellement, l'antiterrorisme a pour fonction de dénicher des fils conducteurs et des motifs à partir de différents types de preuves, il va de soi qu'il puisse avoir recours aux derniers développements des TIC (technologies de l'information et des communications) pour explorer, horizontalement, les données que possèdent en propre tous les organismes distincts compétents. Ce qui, dès lors, soulève des questions quant aux limites institutionnelles verticales qui concèdent aux organismes pris séparément le contrôle exclusif de leurs propres éléments d'information. Jusqu'où le lien entre l'antiterroriste et la révolution de l'information remet-il en question les structures établies des services de renseignements?

Structure du milieu

Dans les pays anglophones, en fait, les structures des milieux du renseignement se sont révélées étonnamment statiques depuis qu'elles ont subi leur dernier grand *façonnage*, juste après la Deuxième Guerre mondiale. Si l'on fait abstraction de l'intégration des diverses équipes des services centraux de renseignements des forces armées, la structure actuelle des services de renseignements britanniques demeure sensiblement la même qu'à l'issue de la guerre, en 1945. Aux États-Unis, depuis la naissance de la CIA (1947) et de la NSA (1952) et exception faite de la mise en place des nouveaux organismes associés aux satellites de renseignement et à l'imagerie qu'ils produisent, l'organisation des milieux du renseignement a accusé un conservatisme relatif. Au Canada, la création du SCRS, indépendant de la GRC, fut sans doute l'une des réformes les plus radicales à s'être produite dans les pays de langue anglaise. Cette relative stabilité a perduré au moment où la réorganisation était endémique dans le reste de l'administration publique et où, partout ailleurs, le mot d'ordre en matière de gestion tournait autour du concept de « souplesse organisationnelle ».

Avant le 11 septembre, nombre d'auteurs américains réclamaient un changement. Dans la majorité des cas, ils exposaient surtout des failles précises : on disait de la National Security Agency qu'elle était fossilisée; on avançait que la nouvelle National Imagery and Mapping Agency n'aurait jamais dû voir le jour; on déclarait que la Defense Intelligence Agency n'avait jamais trouvé réellement sa *vocation*. Aux yeux de certains, la CIA avait un côté civil trop prononcé; pour d'autres, on l'avait trop orientée vers le soutien militaire depuis la guerre du Golfe. Au sommet de la structure, le DCI était jugé inefficace, sans contrôle direct sur l'argent et les postes afférents.

Dans une certaine mesure, une telle conjoncture traduisait la propension des Américains à vouloir améliorer toute chose, mais elle correspondait également à un courant plus vaste, manière de tension s'exerçant sur la pensée organisationnelle. On estimait que la place prise par le renseignement dans

la structure d'organismes distincts et puissants favorisait le cloisonnement, d'où transmission verticale directe, vers le sommet, des données émanant de source unique et intégration insuffisante (données de toutes sources). Les auteurs critiquaient l'espèce de marketing qui en résultait – où on faisait la part belle aux renseignements de source unique au détriment de ceux de toutes sources –, la rivalité entre organismes et la priorité accordée aux intérêts de l'organisme plutôt qu'à ceux du milieu. Le ton était fortement antibureaucratique : les bureaucraties étaient néfastes, les bureaucraties secrètes étaient pires encore[6]. On *lisait* l'avenir du renseignement à travers le prisme de la doctrine organisationnelle moderne prônant la déstratification, les modèles basés sur le marché, les communautés virtuelles et l'esprit d'équipe.

On serait porté à penser que le cloisonnement était devenu un bouc émissaire bien commode, surtout si l'on voulait expliquer des lacunes de toute sorte. Les services de renseignement doivent miser sur une grande fiabilité et des divisions organisationnelles s'imposent si l'on veut nourrir divers types de savoir-faire et de responsabilité. On ne peut abandonner le renseignement à lui-même, accepter qu'il soit partie à la mêlée générale. Un organisme doit assumer la responsabilité première – analyse, contribution aux politiques – dans des situations d'urgence, où il faut réagir rapidement – comme le fait le BSS au Royaume-Uni. (Aux États-Unis, le problème se situe partiellement dans le fait qu'on ne sait pas au juste qui mène la barque, de la CIA ou du FBI, lorsque se trament, à l'étranger, des attaques dirigées contre le territoire national.) La difficulté ne réside pas tant dans l'existence que dans le nombre et l'étendue des cloisons, de même que dans les mécanismes de liaison dont celles-ci sont assorties[7].

Quoi qu'il en soit, on ne peut faire fi de la critique. S'il doit en croire son expérience personnelle (qu'il admet limitée), l'auteur estime que pendant la guerre froide, l'imagerie par satellite des Américains représentait un miracle sur les plans technique et professionnel, mais qu'en raison de son traitement par des organismes distincts dotés de règlements de sécurité différents, il était difficile, pour quiconque, de l'intégrer de façon adéquate aux autres démarches de collecte de données de nature technique. Dans le but de mieux diriger le cheminement de l'information, les services de renseignements ont conçu expressément une manière de labyrinthe, qui ne cesse de se développer, où foisonnent classifications et compartiments spéciaux, une démarche qui se justifiait pendant la guerre froide mais qui nuit à l'efficacité[8]. Après son passage chez les hauts responsables américains, Treverton a eu ce commentaire mémorable voulant que quand on parle de lui (le renseignement) comme d'un *milieu*, on décrit précisément ce qu'il n'est pas : il se situe quelque part entre fiction et aspiration[9].

Ce qui semble particulièrement le cas quand on se penche sur le besoin, pour l'antiterrorisme, de traiter des données de nature diverse. Étonnamment, les analyses des événements du 11 septembre effectuées par les Américains sont restées floues jusqu'à maintenant, mais le cloisonnement – surtout ses effets sur les échanges de renseignements entre la CIA et le FBI – restera incontournable dans toute enquête exhaustive. L'auteur a l'impression que dans les milieux du renseignement de langue anglaise, on maîtrise remarquablement bien les TIC modernes lorsqu'il faut créer des sites Web de renseignements classifiés où sont affichés les rapports rendus publics par les instances compétentes

(produits finaux transmis aux organismes et autres consommateurs de renseignements), mais qu'on ne peut toujours pas prévoir le jour où des analystes sur la trace de terroristes seront à même de puiser automatiquement dans les bases de données inédites des autres organismes.

La réorganisation offrirait à cet égard une réponse simpliste – on pourrait commencer par éliminer la traditionnelle démarcation entre renseignements nationaux et renseignements étrangers. Pareille mesure pourrait ne pas avoir d'effets spectaculaires au Canada, mais en Grande-Bretagne, elle entraînerait la fusion du BSS et du British Secret Intelligence Service (BSIS). Elle s'inscrirait, en principe, dans le phénomène de la mondialisation, qui procure un caractère de plus en plus artificiel aux distinctions entre objectifs étrangers et objectifs nationaux. Les terroristes agissent en partie de l'étranger, en partie de l'intérieur. Ils peuvent se déplacer facilement dans un monde où les voyages à l'étranger sont monnaie courante, où foisonnent les communications planétaires et les finances internationales. Ainsi, une certaine réorganisation axée sur le terrorisme mondial n'est pas tout à fait hors de question. Il est intéressant de se demander si, en 1969, il n'aurait pas été sage pour la Grande-Bretagne de créer, probablement sous l'égide du BSS, un quelconque organisme antiterroriste qui soit plus interdisciplinaire et axé sur les objectifs, si l'on avait su que le terrorisme irlandais allait monopoliser l'attention pour une trentaine d'années.

La réorganisation demeure une solution facile sous certains angles, trop compliquée sous d'autres. Elle ne tient pas compte des compétences propres aux organismes pris séparément et des liens institutionnels entretenus par ces derniers, particulièrement avec leurs pendants à l'étranger. Treverton a habilement décrit la situation : les capacités acquises par les actuels services de renseignements sont à la fois puissantes et difficiles à créer, aussi doit-on y aller avec circonspection lorsqu'on pense à remplacer les entités existantes par quelque chose de nouveau alors qu'on ignore encore la nature exacte du monde qui nous attend[10]. Le 11 septembre n'a pas rendu désuet ce conseil de prudence. Le secteur privé, où la fluidité organisationnelle a valeur de tradition, pourrait bien réussir à se réorganiser, mais il peut courir des risques plus grands que les gouvernements.

Cela dit, il serait surprenant que la Grande-Bretagne opte, un jour, pour la fusion. Les Américains parlent bien de créer, à l'extérieur du FBI, un organisme équivalent au BSS, mais pour ce qui concerne l'intégration des démarches accomplies au pays et à l'étranger, il semble inconcevable que la CIA puisse, un jour, obtenir un mandat l'habilitant à agir au pays – mandat qu'on l'accusait de préparer dans la première moitié de la décennie 1970. Mais qu'importe leur degré d'imbrication, les services de renseignements nationaux et étrangers des pays démocratiques sont assujettis à des restrictions légales et politiques très différentes et il s'y développe, en conséquence, des tournures d'esprit distinctes. Réussir à les fusionner semble difficilement réalisable, voire souhaitable.

Si la réponse (et les mesures correctives) au cloisonnement ne réside pas dans la réorganisation, elle passe par un assouplissement des frontières entre organismes et par le recours aux TIC pour mettre sur pied des milieux virtuels s'étendant à divers organismes. Les permutations entre organismes, la formation interorganismes et d'autres initiatives du genre peuvent contribuer de manière non négligeable à une prise de conscience accrue du milieu. Dans cette optique, le renseignement aurait

peut-être intérêt à s'inspirer des succès remportés par les services des forces armées, qui ont su concevoir des unités opérationnelles communes tout en conservant leur propre identité. Selon un observateur de l'administration publique, la collaboration entre organismes ressortit aux comportements et aux processus plutôt qu'aux structures; la collaboration est un processus à long terme qui, au bout du compte, finit par engendrer un climat dominé par la confiance et la recherche de solutions communes, un climat qui produit ce qu'il appelle une « capacité de collaboration interorganismes »[11] (trad. libre). Si pareille assertion vaut pour tout gouvernement, elle s'applique particulièrement aux services de renseignement, où le secret nourrit un intense sentiment d'appartenance non pas à un milieu, mais bien à un organisme. Les documents traitant du renseignement mettent l'accent sur la nécessité de liens étroits avec les décideurs. Au regard de l'antiterrorisme, pourtant, la grande priorité des organismes de renseignements à source unique reste d'entretenir des liens étroits avec leurs collègues du renseignement de toutes sources, qui envisagent le problème dans son ensemble.

Ce qui fait ressortir l'importance de bons rapports entre les deux volets (source unique/toutes sources). Il faut reconnaître la nature différente des responsabilités qui leur incombent : l'un se spécialise dans les types particuliers de collecte et d'exploitation de renseignements, l'autre agit comme autorité gouvernementale polyvalente sur un sujet donné. La doctrine inhérente aux services de renseignements militaires établit une nette démarcation entre les deux et l'auteur du présent document a déjà écrit que, cette optique aidant, un principe occidental précieux s'est développé – par accident et non à la suite d'une démarche consciente – : normalement, ceux qui recueillent et qui traitent les renseignements ne devraient pas être responsables, au bout du compte, de leur évaluation[12]. Pourtant, les limites institutionnelles entravent ce qui, intellectuellement, est réellement une quête exhaustive de la vérité, idéalement un *jeu sans frontières* (titre d'un concours de chansons d'Eurovision). Malgré l'intérêt de la distinction faite entre renseignements de source unique et renseignements de toutes sources, il n'en demeure pas moins théoriquement artificiel de départager ce qui, en réalité, s'avère une quête perpétuelle de la vérité. Les analystes de renseignements de toutes sources ne disposent pas de faits limpides et objectifs qu'on leur livre tout rôtis dans le bec pour étayer leur recherche. Ils doivent pouvoir s'y retrouver dans le SIGINT et procéder à la démarche inverse[13].

Les données constituant aujourd'hui un actif commun auquel peuvent avoir accès gratuitement des milieux virtuels, les TIC offrent pratiquement la possibilité de concrétiser cette approche face à la recherche de la vérité. En un sens, il s'agit là d'un *desideratum* plutôt évident; certains pourront prétendre que la situation qu'on connaît actuellement n'est pas très loin d'une telle réalité – notamment lorsque les intéressés entretiennent de bonnes relations et sont aiguillonnés par la menace terroriste. D'un autre côté, cette doctrine présente aussi quelque chose de révolutionnaire : elle bouleverse les idées reçues relativement à la protection de la sécurité et aux compétences et responsabilités des organismes spécialisés. Mais nonobstant la pertinence des TIC dans le domaine de l'antiterrorisme, il sera beaucoup plus difficile qu'il n'y paraît, en pratique, d'y avoir recours dans

cette optique. Il faudra un leadership énergique émanant du centre pour réduire les limites interinstitutionnelles sans éliminer le principe de protection de la source. Mais le cas échéant, la question se posera : qui mène quand il est question du renseignement?

Qui mène?

Au cours de la Deuxième Guerre mondiale, le Joint Intelligence Committee (JIC) britannique s'est développé en assumant deux grands rôles associés par ce que l'on pourrait appeler un accident de l'histoire : la direction des services de renseignements du temps de guerre (surtout par voie consensuelle entre les trois services des forces armées) et la production d'évaluations convenues du renseignement à l'intention de ceux qui étaient appelés à prendre les décisions, modèle qu'on a très largement reproduit. La plupart des pays de langue anglaise reconnaissent que des comités contribuent à la production d'évaluations de haut niveau, bien qu'il y ait des différences quant aux rôles précis qui leur sont dévolus. Les comités sont nécessaires à la gestion du renseignement, bien que presque partout ils soient chapeautés par une autorité centrale située quelque part au sein du système. On a noté une tendance générale – moins en Grande-Bretagne qu'ailleurs, cependant – à une séparation des mécanismes de gestion et d'évaluation du milieu. Les deux volets sont toutefois appelés à évoluer davantage. De quelle façon l'antiterrorisme influera-t-il sur leur évolution?

L'un des effets prévisibles peut toucher les deux volets. De par son envergure même et conjuguée aux impératifs de gouvernement moderne – nécessité constante d'une action/réaction immédiate –, la lutte contre le terrorisme a redonné vie à la question posée par Churchill, en 1940, à propos du système britannique : Mais qui donc commande, ici? En Grande-Bretagne comme ailleurs, on ne peut répondre plus clairement à une telle question maintenant qu'alors. Les services de renseignements acquérant de l'importance et les décisions se faisant plus pressantes, les gouvernements et les média se satisferont de moins en moins de réponses qui les renverront à des comités et à des milieux. Ils exigeront un responsable national du renseignement qui soit identifiable. Aux États-Unis, le DCI occupe déjà un tel poste, mais on soutient depuis belle lurette qu'il ne dispose pas, administrativement parlant, du *mordant* voulu; le problème consiste à imaginer des moyens pratiques de les lui donner. En Grande-Bretagne, le président du JIC est le chef en titre du milieu du renseignement, mais on a toujours été des plus hésitants à lui accorder un rôle *proconsulaire* dans un système collégial de nature.

Il existe donc des postes supérieurs pertinents dans les deux systèmes, mais leur influence est, exceptionnellement, tributaire des qualités personnelles de leurs titulaires respectifs et des appuis reçus d'« en haut ». Dans les objectifs présidentiels énoncés récemment, on prévoyait accorder plus de pouvoir au DCI, mais on ne donnait aucun indice sur la façon dont on comptait y parvenir. En Grande-Bretagne, les choses sont plus tranchées. Dans le cadre de la réorganisation *au centre*, Sir David Omand a, récemment, joint les rangs de ce qui fait presque office de dyarchie à l'échelon ultime du Cabinet Office, où il est chargé de la coordination de tous les dossiers relatifs au renseignement et à la sécurité, antiterrorisme compris. Cela ne résout pas le problème de la responsabilité et du soutien ministeriels dans un régime de gouvernement de type britannique, mais

on renforce ainsi assurément le poids du centre au niveau officiel. Les comités ont leur place, mais les menaces terroristes vont vraisemblablement intensifier la tendance, au sein du gouvernement, à cerner les responsabilités personnelles.

Ainsi, dans les deux régimes, et peut-être même dans ceux des autres nations anglophones, l'antiterrorisme pourrait bien avoir pour effet non pas le changement des structures officielles du renseignement, mais l'habilitation *de facto* des titulaires des postes de niveau supérieur évoluant *au centre*. Aux États-Unis, l'actuel DCI, nommé par Clinton, continue à remplir ses fonctions sous l'administration Bush. Doit-on y voir un précédent qui se traduira par une continuité et des pouvoirs accrus? Jusqu'en 2001, au Royaume-Uni, tous les présidents du JIC émanaient du Foreign Office – où leur mission s'assortissait d'autres tâches. S'ils représentaient nécessairement un gain pour le renseignement en raison de leur calibre supérieur, ces gens plein d'avenir avaient aussi tendance à n'être que des oiseaux de passage. Depuis la période qui a précédé immédiatement le 11 septembre, le poste est occupé, et c'est une première, par un professionnel du renseignement à plein temps qui, sans doute, restera en place un bon moment. Les événements s'étant déroulés depuis ont ravivé les impératifs, d'abord formulés en 1947, voulant que le président de cet organisme devait avoir un poste assuré pour une période suffisante et bénéficier d'un personnel de soutien adéquat « s'il voulait insuffler plus de vigueur et donner plus d'influence à l'ensemble de nos services de renseignements »[14] (trad. libre)

Mais son omniprésence aidant, peut-être l'antiterrorisme mettra-t-il en relief le leadership que doit exercer le renseignement et, parallèlement, la nécessité d'une continuité au niveau des fonctions et d'une préparation adéquate du titulaire – préparation échelonnée au fil des postes précédemment occupés. Éventuellement, le dirigeant national du renseignement pourrait jouer un rôle reconnu et être réputé *professionnel* au même titre que les chefs des autres services gouvernementaux spécialisés, ce qui, bien sûr, réduirait l'autonomie des organismes en cause et pourrait soulever des problèmes particuliers; mais le climat de l'après-11 septembre donne à tout le moins aux gouvernements l'occasion d'offrir cette possibilité au milieu. Mais dans un siècle caractérisé par la rapidité du changement, à quoi ressemblera vraiment le milieu du renseignement?

Quel milieu du renseignement?

Le renseignement forme une manière de vaste chapelle; il n'existe pas de définition officielle des dossiers qui lui seraient *interdits*. Le JIC britannique a pour mandat d'évaluer à peu près tout et, lorsqu'il traite de questions qui ne relèvent pas de ses compétences habituelles, il peut s'enrichir de représentants d'autres services. Mais en pratique, c'est lorsqu'il a à traiter d'éléments ressortissant aux menaces, aux mises en garde, à la violence, aux troubles internationaux et à la guerre qu'il est le plus dans son élément et que son influence est la plus forte. Washington a eu tendance à adopter une vision plus large (ex. : la production, par la CIA, d'études de prospective sur les tendances mondiales). Mais au moins jusqu'à la fin de la guerre froide, on admettait généralement, dans les

pays de langue anglaise, que les services de renseignements étaient des plus utiles pour tout ce qui relevait, d'une façon ou d'une autre, de la sécurité nationale, plus facilement définie dans un contexte intérieur que dans un contexte extérieur.

Ce tableau d'ensemble a subi certaines modifications dans la décennie 1990. On s'est intéressé au renseignement de nature économique, secteur qu'on estimait en pleine croissance et qui, au bout du compte, n'a pratiquement pas bougé. En évolution, les liens entre le renseignement et les autorités chargées de l'application des lois, surtout les services de police, d'immigration et des douanes, se sont révélés plus prometteurs. Ils n'étaient pas nouveaux en soi, mais on les a étoffés, à la fois au Royaume-Uni et aux États-Unis, pour permettre aux organismes de renseignements de bonifier la collecte de données sur le trafic des stupéfiants, le blanchiment d'argent et d'autres activités liées au crime organisé, notamment à l'échelon international. Les stupéfiants sont devenus un domaine d'intervention incontournable pour la CIA et, en matière de collecte, la grande priorité du JIC, qui a d'ailleurs produit des rapports sur le sujet. Selon des médias, le BSS aurait été chargé de fouiller les aspects occultes de la corruption au sein des services de police et le BSIS aurait hérité de la tâche de pister ceux qui organisaient l'immigration illégale, élément qui a également glissé dans la sphère d'activité du JIC. Parfois, même, on a mis le renseignement militaire à contribution pour fouiller des activités criminelles, comme ce fut le cas en Bosnie et au Kosovo, lorsque les forces de maintien de la paix ont eu besoin de se renseigner sur la mafia locale et internationale.

Parallèlement, le renseignement lui-même se transformait, en quelque sorte, en un nouveau champ de spécialisation au sein même des organismes d'application de la loi. En Grande-Bretagne, des indices portaient à croire qu'il donnait naissance à une communauté propre, dirigée et coordonnée par le nouveau National Criminal Intelligence Service (NCIS). Dans ce pays, à tout le moins, le « maintien de l'ordre par le renseignement » est devenu le leitmotiv qu'on ressert à tout propos pour réclamer une meilleure efficacité de la police. On reconnaît les intérêts communs entre l'ancien et le nouveau milieux du renseignement à la participation du NCIS aux réunions du JIC. Tant au Royaume-Uni qu'aux États-Unis, les organismes de renseignements existants procèdent à des échanges de données sur le crime international avec les services qui ont succédé au KGB dans l'actuelle Russie. Ainsi, même avant le 11 septembre, il y avait place aux suppositions quant aux futures démarcations entre nouvelle et ancienne fournées du renseignement et à la possibilité qu'à long terme, les deux volets en arrivent à fusionner, surtout dans l'optique où les crimes complexes débordaient de plus en plus les frontières des États pour devenir internationaux, tout spécialement en Europe et probablement dans les deux Amériques.

L'antiterrorisme vient encore nourrir pareille hypothèse. Il donne lieu à une étroite coopération entre les deux ensembles d'organismes particulièrement importants. Les forces de police contribuent au premier chef au renseignement sur le terrorisme et comptent parmi ses premiers consommateurs. Mentionnons qu'en Grande-Bretagne, l'analyse du financement du terrorisme est avant tout l'affaire du NCIS, que les effectifs du National Counter Terrorism and Security Office proviennent tant des services de police que du Security Service et que des représentants de ce dernier font partie intégrante de la Police International Counter Terrorist Unit. Aux États-Unis, la nécessité d'une

meilleure coopération de cette nature figurait parmi les thèmes du message annuel du président – message dont on a déjà parlé. En règle générale, les terroristes ne sont pas des criminels au sens propre du terme, mais l'infrastructure même à laquelle ils sont assujettis les rend susceptibles de participer à diverses formes d'activités criminelles et d'actes illégaux.

Bien sûr, toute démarche officielle visant l'intégration et l'utilisation à diverses fins des renseignements personnels que détiennent les gouvernements sur leurs ressortissants soulève de grandes questions de principe. Une manière d'« anxiété libertaire » entoure le programme américain de recherche *Total Information Awareness*, dans le cadre duquel on envisage de retracer les terroristes en appariant, entre autres choses, passeports et demandes de visa, dossiers criminels et scolaires, registres des logements, renseignements sur les voyages et sur les transports et, finalement, données indissociables de l'identité personnelle (empreintes digitales et rétiniennes, par exemple). Même s'il n'est pas relié à la sécurité, l'objectif que poursuit l'actuel gouvernement britannique – recourir aux TIC pour établir des liens entre les divers services qu'il offre aux citoyens (ou, si l'on veut, mettre en place un « gouvernement intégré ») – a soulevé des craintes semblables à celles qu'a illustrées Orwell dans *1984*. En termes institutionnels, la nécessité de contrer le terrorisme pourrait bien, pourtant, nous inciter à étoffer les milieux traditionnels du renseignement en étendant leur représentation et leurs responsabilités au domaine de l'application de la loi.

Même dans le contexte d'une révolution de l'information, de telles modifications d'envergure n'iraient pas sans soulever des objections substantielles. La différence fondamentale est indissociable d'une part de la principale préoccupation des services de police, soit la perpétration d'activités criminelles dites « normales » en vue d'en tirer un profit financier et, de l'autre, du recours à la violence, par les terroristes, pour arriver à des fins politiques. En Grande-Bretagne, il serait surprenant que le JIC en vienne à intégrer, comme membre à part entière, le NCIS et d'autres organismes d'application de la loi et qu'on lui confie un jour, entre autres responsabilités permanentes, d'importants secteurs de la répression de la criminalité, ce qui serait d'ailleurs, tout compte fait, peu souhaitable et peu probable. D'un autre côté, l'expérience américaine – qui fait apparaître la nécessité de mettre en commun renseignements étrangers et données nationales – semble si convaincante qu'il serait étonnant que la création du nouveau Département de la sécurité intérieure ne donne pas lieu à des bouleversements. Chose certaine, l'antiterrorisme accentue l'interdépendance du (vieux) milieu du renseignement et de son (nouveau) vis-à-vis du champ d'application de la loi. Le renseignement traditionnel a toujours eu des frontières quelque peu floues et les impératifs associés à l'application de la loi et à l'antiterrorisme ne viennent pas clarifier les choses.

Une dimension internationale, d'accord... mais jusqu'où?

Même si l'on fait abstraction de la contribution aux volets étrangers et nationaux d'application de la loi, force est de reconnaître que la collaboration avec l'étranger avait acquis de plus en plus de place dans les activités normales des services de renseignements avant le 11 septembre. Évidemment, les liens avec l'étranger n'ont rien de neuf : ils constituaient déjà une caractéristique

non négligeable des alliances occidentales du temps de la guerre froide et on les a approfondis dans les années 90. Le terrorisme international constituait déjà, alors, un objectif prioritaire. Les interventions gouvernementales mettant à contribution l'aspect militaire se faisaient aussi de plus en plus multilatérales de nature – comme dans l'ex-Yougoslavie – et s'articulaient de façon croissante autour du renseignement. Il en allait de même des efforts internationaux visant à surveiller et à contrer la mise au point des armes de destruction massive et autres menaces. Il y a eu, par la suite, mise en commun de plus en plus grande des renseignements. Avant le 11 septembre, la CIA entretenait déjà des relations avec 400 organismes de renseignements et de sécurité étrangers. À la même époque, le FSB russe (l'ex-KGB, équivalent du SCRS) affirmait que quelque 80 missions représentant les services spéciaux de 56 pays oeuvraient en permanence à Moscou et qu'il avait conclu des ententes officielles avec 40 partenaires étrangers dans 33 pays[15]. Jusqu'à ce qu'elle se retire de l'Irak, en 1998, la CSNU aurait, dit-on, obtenu des renseignements de quelque vingt pays sur le non-respect des sanctions et la mise au point d'armes par l'Irak.

Mais les événements du 11 septembre ont survolté cette internationalisation. Ils ont convaincu les États-Unis que même s'ils étaient une superpuissance en matière de renseignements, ils ne pouvaient, seuls, réussir à contrer le terrorisme. Pratiquement chaque nation est capable de fournir des renseignements uniques sur le terrorisme mondial en mettant à profit dossiers nationaux et sources humaines et techniques – qu'on pense, simplement, à l'écoute téléphonique. Dans la résolution 1373 adoptée immédiatement après le 11 septembre, le Conseil de sécurité demandait expressément qu'on procède à de tels échanges – que, dans le style onusien, on associait encore à l'« information ». Les États-Unis ont noué un réseau de nouvelles relations antiterroristes. La Grande-Bretagne a fait de même, comme en témoignait, notamment, l'annonce Blair-Poutine de décembre 2001 concernant la mise en place d'un nouveau mécanisme anglo-russe pertinent. Un an plus tard, en septembre 2002, le message du président confirmait officiellement que les Américains entendaient coordonner étroitement leurs démarches avec leurs alliés en vue d'en arriver à une évaluation commune des menaces les plus dangereuses. Le BSS, l'organisme britannique qui est obligatoirement le plus tourné vers l'intérieur, disait disposer, à l'étranger, de plus d'une centaine de liens[16].

Le passage vers une meilleure coopération n'a pas toujours été constant. Oscillant entre deux pôles – le premier incitant à solliciter le soutien international et l'autre à faire cavalier seul –, les politiques américaines influent à n'en pas douter sur le climat des services de renseignements, comme sur tout le reste. Depuis le 11 septembre, quoi qu'il en soit, l'intensification de la collaboration intergouvernementale des services de renseignements, parfois entre alliés improbables, a bouleversé du tout au tout ce qu'on avait jusqu'alors tenu instinctivement, malgré les liens avec l'étranger, pour une activité nationale fondamentalement isolée, s'exerçant dans la réclusion, profondément ancrée dans le secret et ressortissant aux intérêts nationaux (une manière de match spécial à somme nulle entre États, axé sur le renseignement, à cent lieues, en un sens, de la trame officielle des relations internationales ou, si l'on veut, le « fait de gens spéciaux évoluant dans des cases spéciales »). Par contraste, la collaboration entre les services de renseignements fait, désormais, aussi souvent la manchette des médias que les anciens éléments des relations internationales.

Dès lors, la coopération ajoute peut-être un autre facteur à l'évolution radicale du concept sous-tendant le renseignement pris dans son ensemble. Les événements du 11 septembre ont mis en relief les aspects cachés et la nécessité du secret, mais ils doivent aussi avoir renforcé la tendance, déjà apparente dans les années 90, à s'éloigner du ciblage gouvernemental de ce que l'ère victorienne appelait les « États civilisés » pour se concentrer plutôt sur des entités non étatiques – y compris des organisations terroristes –, sur des États et situations posant problème, sur des États parias qui déparent l'échiquier international (surtout ceux qui appuient ou qui abritent le terrorisme). L'importance qu'on accorde aux unités formant cette nouvelle catégorie – dont Al Qaida, l'Irak et la Corée du Nord sont des exemples types – a pour corollaire une réduction de la couverture des États « normaux », couverture qui constitue ce fameux adjuvant de la diplomatie et des négociations classiques ou, encore, le « dix pour cent » qu'ajoute le renseignement clandestin aux rapports diplomatiques réguliers, selon un éminent diplomate britannique.

De là s'est concrétisée la possibilité d'un nouveau paradigme pour les services de renseignements. Dans le système international composé d'États (normaux), le renseignement se transforme pour devenir non plus une lutte à somme nulle, mais une activité de coopération dirigée contre des menaces/préoccupations communes. Même les grands désaccords de nature politique – comme, au moment de la rédaction du présent texte, au regard des mesures à prendre face au refus de Saddam Hussein de se plier aux inspections de l'ONU – reposent sur des preuves mises en commun (ou partiellement mises en commun). Le renseignement fournit désormais la matière première aux discours publics et intergouvernementaux à l'échelle de la planète. En matière de renseignement, le paradigme de la coopération (au niveau des activités et de l'interprétation) se voulait implicite dans les faits nouveaux qui ont émaillé les années 90, mais, à la lumière des événements du 11 septembre et de ceux qui ont suivi, il nous est désormais loisible de l'orchestrer.

On a débattu, ailleurs[17], des résultats possibles de l'existence de ce nouveau paradigme pour ce qui touche à la collecte de renseignements à l'échelle internationale et à l'acquisition d'une capacité d'analyse multilatérale et mondiale. Il y a déjà eu des activités de collecte sous l'égide de l'ONU : unités tactiques des Casques bleus au Congo, opérations dans l'ex-Yougoslavie, sorties des U-2 américains au-dessus de l'Irak sous contrôle de la CSNU et de la COCOVINU. Mais il est peu probable que cette orientation devienne la principale tendance. Pour la plus grande part, les activités de collecte de renseignements demeureront nationales, mais elles s'assortiront d'éléments internationaux plus officiels – la mise en commun des renseignements et l'analyse des résultats, par exemple. Le milieu du Royaume-Uni/États-Unis/Commonwealth dispose depuis longtemps d'arrangements prévoyant la participation commune à des démarches d'appréciation des renseignements (à l'instar du JIC). Il n'existe aucune raison intrinsèque qui empêcherait le Conseil de l'Atlantique Nord de disposer d'un mécanisme semblable regroupant une équipe internationale du renseignement. Rien n'interdirait non plus au Conseil de sécurité d'avoir pareil instrument à sa disposition, encore que dans ce cas précis, il faudrait parler d'« analyse » et non de « renseignement ». Aujourd'hui (13 février), on rapporte que la COCOVINU a convoqué en réunion

de spécialistes des missiles de six pays qui, de concert avec sa propre équipe d'analystes, évalueront les preuves de l'existence des missiles irakiens. Ne peut-on voir là une équipe d'évaluation internationale *de facto*?

Le développement d'un tel mécanisme officiel, axé sur la coopération, semble utopique : non seulement assimile-t-on encore trop le renseignement à une chasse gardée nationale, mais encore cela supposerait : que les États acceptent de réduire encore l'importance de la collecte intrusive les uns par rapport aux autres, reconnaissant qu'une sorte de « contrôle du renseignement » faciliterait la coopération et libérerait des ressources – qu'on pourrait consacrer à de nouveaux objectifs –, que le renseignement n'est pas automatiquement associé à des activités secrètes et que les gouvernements du monde entier en viendraient à escompter une manière de sincérité professionnelle des services de renseignements et cesseraient de les tenir pour des instruments politiques. Le KGB voyait dans la collecte de renseignements une forme spécifique de lutte politique utilisée par les organismes de renseignements d'un État pour aider celui-ci à s'acquitter de ses fonctions internes et externes[18]. Dépouillée de son idéologie, cette façon de voir est encore largement répandue dans le monde. Peu de gouvernements ou de grands publics croient que le renseignement n'est pas qu'un simple moyen d'intervention politique ou d'exploitation du pouvoir.

Au fil du temps, cependant, les nations et leurs leaders peuvent modifier presque du tout au tout leurs hypothèses de travail. Au sein du monde du renseignement lui-même, les moyens techniques nationaux de collecte de l'information (euphémisme qui désigne le SIGINT et l'imagerie) ont vu leur cote de légitimité s'accroître de façon absolument imprévisible dans le cadre du contrôle des armements stratégiques américano-soviétiques pendant la guerre froide et des accords internationaux ultérieurs[19]. Avant le Siècle des lumières (le XVIII^{e} siècle), la guerre entre États était, de façon générale, une activité presque automatique, inscrite dans l'ordre naturel des choses. C'est sans doute à Kant que revient l'honneur d'avoir perçu que la paix pouvait être autre chose qu'une pieuse aspiration[20]. Au XIX^{e} siècle, la Croix-Rouge s'est développée dans le sillage d'une initiative privée qui, gagnant en popularité, a fait bouger les gouvernements[21]. La Conférence de la Haye, en 1899, qui a fortement contribué au droit de la guerre, découlait d'une démarche inattendue du Tsar, qui réagissait sans doute à la lecture d'un ouvrage sur les guerres de l'avenir[22]. Les vues du pouvoir militaire lui-même amorcent une mutation semblable. Par exemple, la vision où l'auteur (britannique) imagine des soldats professionnels de la démocratie contrant la violence au nom de la société internationale, « ... d'honorables guerriers recourant à la force au nom de la paix »[23] (trad. libre). Sous réserve des ajustements qui s'imposent, la menace terroriste éveille une perspective similaire du renseignement. Ainsi, tout comme les événements du 11 septembre ont amené les gouvernements à alléger les barrières à l'information au sein de leurs propres systèmes nationaux pour améliorer la coopération entre organismes, ils ont fait ressortir la nécessité d'envisager le renseignement davantage dans une optique commune de coopération internationale.

Conclusion

Le 11 septembre 2001 a fait du renseignement antiterroriste une priorité incontournable, que nous ne pourrons respecter que dans un climat d'intensité qui s'apparente presque à celui du temps de guerre. Cette priorité ne sera pas transitoire et aura une grande incidence sur la nature mondiale du renseignement. Parallèlement, ce dernier s'inscrit dans la révolution des technologies de l'information et des communications (TIC), une révolution qui, bizarrement, arrive à point nommé si l'on veut satisfaire aux besoins, propres à l'antiterrorisme, de détection de liens dans de vastes plages d'information où se côtoient maints types de données. Une révolution qui, enfin, modifie aussi les organismes, les relations et les milieux d'une façon plutôt radicale. Vouloir en tirer pleinement profit dans la lutte contre le terrorisme remet obligatoirement en question les structures et les frontières – déjà vieilles – des services de renseignements et le cloisonnement qu'elles suscitent.

Face au terrorisme international, il pourrait sembler logique de procéder à une réorganisation où l'on fusionnerait, en un seul organisme axé sur les TIC, tous les services de renseignement étrangers et de renseignements de sécurité afférents, mais une telle démarche serait, en fait, superficielle. Le remède au cloisonnement réside plutôt dans des adaptations culturelles de divers types visant à favoriser une conscience accrue du milieu du renseignement, élément indispensable au développement de systèmes des TIC enjambant les frontières entre organismes. Promouvoir cette prise de conscience exigera du leadership de la part des services centraux de renseignements, tout comme la nécessité de tenir compte du rythme affolant avec lequel doivent composer les gouvernements modernes et de satisfaire aux demandes de ceux-ci en matière de renseignement. Les comités continueront à avoir leur place, mais les gouvernements s'attendront de plus en plus à ce que les principaux responsables de leurs services de renseignement soient dotés de la pleine et entière responsabilité pour ce qui touche à leur milieu national du renseignement.

Ces milieux eux-mêmes subiront des transformations qui obéiront à d'autres impulsions. La lutte contre le terrorisme mettra en relief le caractère indispensable de liens accrus avec les services d'application de la loi et leur nouveau milieu du renseignement spécialisé et, sous un autre aspect, les services qu'elles offrent acquerront une dimension qui ira en s'internationalisant. Ils resteront des institutions nationales, mais on les assimilera de plus en plus à des piliers de la coopération entre États en vue de la réalisation d'objectifs communs – surtout mais pas exclusivement afférents à la lutte contre le terrorisme. Il s'agira, en un sens, d'une ligne de défense dont disposeront les États pour contrer les menées d'ennemis non étatiques. Ils demeureront profondément influencés par la nécessité du secret inhérente à l'antiterrorisme tout en étant, parallèlement, adaptés au besoin d'une collaboration transfrontalière/sectorielle accrue – avec les intervenants de leur propre milieu, avec les organismes d'application de la loi et d'autres entités actives dans la lutte au terrorisme, avec leurs homologues étrangers et avec les responsables des mécanismes d'évaluation spécialisés de l'OTAN, de l'ONU et d'autres plafeformes régionales et internationales.

Renvois

1. Bruce D. Berkowitz et Allen E. Goodman, *Best Truth: Intelligence in the Information Age*, New Haven et Londres, Yale University Press, 2000, p. 98.

2. *Security Monitor* (RUSI Londres), premier numéro, 2002. Les citations sont tirées de cet article.

3. Gregory F.Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge University Press, 2001.

4. Michael Herman, *British Intelligence towards the Millennium*, Londres, Centre for Defence Studies, pp.64-65.

5. S. Rimington, Richard Dimbleby, conférence, *Security and Democracy*, Londres : BBC Educational Developments, 1994, p. 9.

6. Allocution de Robert Steele, St Antony's College Oxford, 12 juin 2002.

7. Je suis reconnaissant à feu le colonel Kevin Cunningham, US Army War College, pour ses commentaires éclairés.

8. L'actuel Secrétaire américain à la défense se serait plaint du fait qu'une séance d'information sur la défense nationale antimissile tenue récemment était chaotique, car aucun analyste n'était en mesure de présenter une vue globale, et ce, en raison du compartimentage.

9. Treverton, p. xiii.

10. Treverton, p. 249.

11. E. Bardach, *Getting Agencies to Work Together: the Practice and Theory of Managerial Craftsmanship*, Washington, Brookings Institute, cité par Wayne Parsons, « Modernising Policy-Making for the Twenty-First Century: the Professional Model », *Public Policy and Administration*, vol. 16, n° 10 (automne 2001).

12. Michael Herman, *Intelligence Power in Peace and War*, Cambridge, Cambridge University Press, 1996, p. 112.

13. Michael Herman, *Intelligence Services in the Information Age*, Londres, Cass, 2001, p. 193.

14. Rapport Evill de 1947 sur le JIC, cité dans *Intelligence Services in the Information Age*, p. 114.

15. Article du directeur du FSB, N. Patrushev, Service national de l'information de la Russie, 20 décembre 2001.

16. *MI5 : The Security Service*, publication officielle, quatrième édition, 2002, p. 26.

17. Michael Herman, « 11 September: Legitimizing Intelligence? », *International Relations*, vol. 16, n° 2 (août 2002).

18. Vasiliy Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, Londres, Cass, 2002, p. 200.

19. Survol historique dans *Intelligence Power in Peace and War*, pp. 159-62.

20. Citations de M. Howard, *The Invention of Peace: Reflections on War and International Order*, Londres, Profile Books, 2000, pp. 13 et 31.

21. Pam Brown, *Henry Dunant : les gens qui ont aidé l'humanité*, Montréal, L'Étincelle, 1989.

22. G. Best, « Peace Conferences and the Century of Total War: The 1899 Hague Conference and What Came After », *International Affairs*, vol. 75, n° 3 (juillet 1999), p. 622.

23. Conclusion dans J. Keegan, *War and Our World*, Londres, Hutchinson, 1998 (Conférences Reith de 1998), p. 74.

Michael Herman (MHe24@aol.com) a été au service du gouvernement britannique de 1952 à 1987. Il collabore aujourd'hui avec l'Université d'Aberystwyth et avec le College Oxford de St Antony. Il a publié *Intelligence Power in Peace and War* (1996) et *Intelligence Services in the Information Age* (2001).

Commentaire est publié régulièrement par la Direction de la recherche, de l'analyse et de la production du SCRS. Si vous avez des questions sur la teneur du document, veuillez vous adresser au directeur général de la Direction de la recherche, de l'analyse et de la production à l'adresse suivante : C.P. 9732, Succursale « T », Ottawa (Ontario), K1G 4G4; ou par télécopieur au (613) 842-1312. Consultez notre site Internet pour les numéros antérieurs de *Commentaire* : http://www.csis-scrs.gc.ca

ISSN 1192-277X
Catalogue JS73-1/83